AO 106 (Rev. 5/85) Affidavit for Search Warrant

United States District Court

DISTRICT OF Delaware

REDACTED

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

[redacted] Dagsboro DE 19939

described more particularly on Attachment A

APPLICATION AND AFFIDAVIT FOR WARRANT

CASE NUMBER: 06-90M-MPT

I SA David B. Yeary, ICE being duly sworn depose and say:

I am a(n) Special Agent, Immigration and Customs Enforcement and have reason to believe
Official Title

that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

[redacted] Dagsboro DE 19930, described more particularly on Attachment A

in the _____ District of Delaware .

there is now concealed a certain person or property, namely (describe the person or property)

see Attachment B

which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of a crime and contraband

in violation of Title 18 United States Code, Section(s) 2252 and 2252A

The facts to support the issuance of a Search Warrant are as follows:

see attached affidavit

FILED
MAR 13 2007
U.S. DISTRICT COURT
DISTRICT OF DELAWARE

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant
SA David B. Yeary, ICE

Sworn to before me, and subscribed in my presence

8/9/06 at Wilmington, DE

Date City and State

Honorable Mary Pat Thynge
United States Magistrate Judge

Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

[redacted] **Dagsboro DE 19939** (the "SUBJECT PREMISES"), which is more particularly described as white two-story single family residence, with a mailbox on the street with the number "200 on the mailbox and on the pole supporting the mailbox. There is also the letters "DERR " on the mailbox.
The front of the house has a wooden porch leading to the front door. The front door is white in color with a window on each side of the door. The garage for the house is on the left side of the house.

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

a. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256. Said records are to include

communication with dykstra@hotmail.com account, and access to http://mhumbu.badlink.net; http://pliac.hotfire.net, and; http://hualama.cjb.net.

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. credit card information, including but not limited to billing and payment records, for all credit and check card accounts, including the check card account of Delaware National Bank, account #4194 3500 0017 5858, issued to Brad Derrickson;

d. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

e. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access (to include Mediacom Communication Corp.), and handwritten notes.

I, David B. Yeary, being duly sworn, depose and state:

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), assigned to the Resident Agent in Charge in Wilmington Delaware. I have been so employed since January 2003. As part of my daily duties as an ICE agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)[1] in all forms of media including computer media. I have also participated in the execution of search warrants many of which involved child exploitation and/or child pornography offenses.

2. This Affidavit is made in support of an application for a warrant to search the entire premises located at [redacted] Dagsboro DE 19939 a single family residence (the SUBJECT PREMISES). The SUBJECT PREMISES to be searched is more particularly described in attachment "A". The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess, or attempt to possess, child pornography, and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which

---

[1] "Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging

make it a crime to receive, or attempt to receive, child pornography in interstate commerce by computer.

3. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted and based on my conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography.

4. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located at the SUBJECT PREMISES and within a computer and related peripherals, and computer media found at the SUBJECT PREMISES. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

5. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, are present at the SUBJECT PREMISES.

6. The instant investigation has revealed that an individual employing the e-mail account "n3wau@mchsi.com", subsequently identified as Brad Derrickson purchased at least one subscription to a website that was distributing child pornography, and that there is probable cause to believe that Brad Derrickson subscribed to this website using a computer that is located at the SUBJECT PREMISES.

7. Paragraphs 8 and 9 explain technical terms and concepts related to computers.

---

in sexually explicit conduct." 18 U.S.C. § 2256(8).

Paragraphs 10 through 12 explain how computers and computer technology have revolutionized the way in which child pornography is produced, utilized and distributed. The information set forth in paragraphs 13 through 25 provide background concerning an underlying investigation through which the lead to the SUBJECT PREMISES was developed. They also provide a general overview of how subscriptions to a particular website labeling itself "Illegal CP" and offering access to child pornography were linked to individual purchasers including a purchaser that is believed to reside at the SUBJECT PREMISES. Finally, paragraphs twenty six (26) through thirty-five (35) describe, more particularly, the investigation of the SUBJECT PREMISES.

THE INTERNET AND DEFINITIONS OF TECHNICAL TERMS PERTAINING TO COMPUTERS

8. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers[2] and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive

[2] **Computer**: The term "computer" is defined by 18 U.S.C. § 1030(e)(1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a commercial service – which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, whether from a residence, a university, or a place of business, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see definition of "websites" below), and make purchases from them.

9. Set forth below are some definitions of technical terms, many of which are used throughout this Affidavit, and in Attachments A and B hereto, pertaining to the Internet and computers more generally.

a. **Client/Server Computing**: Computers on the Internet are identified by the type of function they perform. A computer that provides resources for other computers on the Internet is known as a **server**. Servers are known by the types of service they provide - that is - how they are configured. For example, a **web server** is a computer that is configured to provide web pages to other computers requesting them. An **e-mail server** is a computer that is configured to send and receive electronic mail from other computers on the Internet. A **client computer** is a computer on the Internet that is configured to request information from a server. If a client computer is configured to browse web pages and has web page browsing software installed, it is considered a **web client**.

b. **Computer system and related peripherals, and computer media**: As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and

MPEG.

c. **Domain Name**: Domain names are common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the United States government, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

d. **Internet Service Providers (ISPs) and the Storage of ISP Records**: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of services for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers (defined below) and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("**ISP records**") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended

recipient, usually within an area known as the home directory or mailbox. Such temporary, incidental storage is defined by statute as "**electronic storage**," see 18 U.S.C. § 2510(17), and the provider of such a service is an "**electronic communications service.** " An "**electronic communications service,**" as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "**remote computing service.**" 18 U.S.C. § 2711(2).

e. **Internet Protocol Address (IP Address)**: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ **dynamic IP** addressing - that is - they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A **dynamic IP address** is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISP's, including some cable providers, employ **static IP** addressing - that is, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a **static IP address** is an IP address that does not change over a period of time and is typically assigned to a specific computer.

f. **Log File**: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. **Modem**: A modem is an electronic device that allows one computer to communicate with another.

h. **Trace Route**: A trace route is an Internet debugging tool used to document the list of inter-connected computers between two computers on the Internet. A trace route will list the names and IP addresses of computers that provide the physical link between two computers on the Internet. Trace routes are useful tools to help geographically identify where a computer on the Internet is physically located, and usually includes information about the registered owner of computers on the Internet.

i. **Universal Resource Locator (URL)**: A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web's browser address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

j. **Website**: A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

k. **Website Hosting**: Website hosting provides the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. "**Dedicated hosting**" means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "**Co-location**" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, climate control, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft, or vandalism is greater.

COMPUTERS AND CHILD PORNOGRAPHY

10. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership and subscription-based websites to conduct business, allowing them to remain relatively anonymous.

11. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child

pornography in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number or otherwise directly connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child

pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache[3] to look for "footprints" of the websites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 40 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

12. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack

[3] "Cache" refers to text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

OVERVIEW OF THE NEW JERSEY INVESTIGATION

13. The information set forth below is provided as a broad overview of the investigation conducted to date. It does not include a listing of all investigative techniques employed or even the full and complete results of any of the listed investigative efforts.

14. The United States Attorney's Office for the District of New Jersey ("USAO DNJ"), and the New Jersey offices of ICE have conducted an investigation (the "New Jersey Investigation") of a commercial website labeling itself "illegal.CP" (hereinafter the "Illegal CP" website)[4] which offers access to thousands of images and videos of child pornography via subscriptions of 20 and 30 days' duration. The investigation has revealed that the owners and operators of the "Illegal CP" website have conspired with other corporate entities and individuals, including the operators of a company known as "AD-SOFT" to commercially

[4] The term "CP" is an abbreviation commonly used on the Internet to denote "child

distribute child pornography.

A. The Investigation of the "Illegal CP" Website

15. In or about October 2005, agents with ICE located a website known as the "Illegal CP" website at a URL of http://hualama.cjb.net/, accessible via the Internet at that time through another web page located at a URL of http://deadundead.info/main.html, which was accessible via the Internet, including from New Jersey. The banner page of the website -- that is, the page which initially appeared and which did not require the person accessing the website to provide any financial or personal information - labeled itself "illegal.CP," and featured more than one dozen images of what appear to be minors engaging in sexual acts with other minors or adults.[5] The banner page further proclaims that "[n]ow you are in [sic] few minutes away from the best children porn site on the net!" The banner page further stated that "[i]f you join this site you will get tons of uncensored forbidden pics (over 5 at this moment), forbidden stories, and, of course, many videos." The banner page also featured purported feedback from a self-described pedophile who praised the website. The words "join now" appear at the top and bottom of the page.[6]

16. On or about October 26, 2005, an ICE agent, acting in an undercover capacity,

---

pornography."

[5] The banner page was actually part of the "deadundead" web page on October 26, 2005. This banner page, through which ICE agents obtained a subscription to the "Illegal CP" website, was captured and preserved by agents. Once a user clicked upon the "Join Now" button, a page requesting personal and credit card information appeared. This page was also technically part of the "deadundead" website. After entering the requested financial information, the user would receive e-mail confirmation of the purchase as well as a login and password to access the "Illegal CP" website.

[6] The content of the banner page itself was not located on the server containing the contents of the "Illegal CP" website, which was maintained during October and November 2005 on a server

(hereinafter UC-1) purchased access to the "Illegal CP" website after accessing this banner page. On October 27, 2005, an e-mail from theodore_dykstra@hotmail.com was received at the undercover e-mail address established by ICE agents. That e-mail provided UC-1 with a login and a password to a URL of http://hualama.cjb.net/. The e-mail message also indicated that the credit card charges would appear on UC-1's credit card bill as "ADSOFT" and would include a charge for $79.99.

17. Upon entering the login and password provided via the e-mail from theodore dykstra@hotmail.com, UC-1 was able to gain access to the "Illegal CP" website. The login and password block stated that UC-1 was being connected to the IP address of "72.29.83.114." Upon accessing the website, a URL of http://hualama.cjb.net appeared. The top of the initial page which appeared upon entry into the website stated as follows:

> FAQ, Please read. "Our site is considered to be illegal in all countries.... Even if you ever have problems with police, you can always say that someone had stolen the information from your credit card and used it. It is very difficult to establish that you were the person to pay."

18. Upon examination of the contents of the website, ICE agents determined that it contained thousands of what appeared to be images of child pornography. Upon placing the cursor over a particular image, a URL was listed at the bottom of the screen of "72.29.83.114/~medialo/1/index.html." The website contained both still images and videos of child pornography, and offered the purchase of additional videos through the website. For example, three of the still images of child pornography found on the "Illegal CP" website are described as follows:

---

located in Orlando, Florida, but on another server located in California.

a. http://72.29.83.114/~medialo/1/pics/300/0013.jpg: This image depicts a nude, adult male sitting upon a floor with his legs spread wide apart. A nude, prepubescent female is also depicted, and she is lying on her back with her legs spread apart. The left hand of the male is holding the female's right leg. His erect penis appears to be penetrating the prepubescent female's vagina.

b. http://72.29.83.114/~medialo/1/pics/300.0022.jpg: This image depicts a nude prepubescent female in a standing position. She is facing an adult male who also appears to be standing. The male is wearing what appears to be a dark-colored robe, but his genital area is exposed. The prepubescent female has her left hand wrapped around the male's penis and appears to be performing fellatio upon him.

c. http://72.29.83.114/~medialo/1/pics/300/0073.jpg: This image depicts what appears to be an adult male wearing a white shirt who is nude below the waist. He appears to be lying upon a bed with red pillows. A nude, prepubescent female is sitting upon the bed next to the male. Her legs are bent so that her buttocks rests on her feet. Her right hand is holding the male's penis.

19. Through the use of a commercially available search tool, law enforcement agents were able to determine that the IP address listed for the "Illegal CP" website – 72.29.83.114 – was associated with a server based in Orlando, Florida, which hosted the content of the "Illegal CP" website during October and November 2005. The search tool revealed that the server is owned by HostDime.com, Inc., 111 N. Orange Avenue, Suite 1050, Orlando, Florida. This information was verified on or about November 14, 2005, and a representative of HostDime.com confirmed that it was in possession of the server in question on or about November 16, 2005.

20. A search of the server on which the contents of the "Illegal CP" website were maintained was performed on or about November 17, 2005 pursuant to a court-authorized search warrant. A review of the contents of this server revealed the presence of thousands of images and videos of child pornography. Further, a review of the contents of the server revealed the IP address for all contacts with the content maintained

on the server (the "Illegal CP" website) that had occurred from on or about November 9, 2005 through on or about November 17, 2005. Specifically, this data revealed that hundreds of IP addresses presumably associated with individual subscribers had visited the "Illegal CP" website during this nine-day period. The data also demonstrated which individual images had been accessed by each IP address. On or about December 14, 2005 and January 5, 2006, two additional search warrants were executed on the HostDime server on which the contents of the "Illegal CP" website were hosted through December 2005. Both searches produced additional log files documenting contacts from specific IP addresses with particular images contained on the "Illegal CP" website. During November and December 2005, it is believed that the operators of the "Illegal CP" website shifted the location of the contents of the "Illegal CP" website to a different server and began phasing out the use of the HostDime.com server.

21. On or about December 23, 2005, the Honorable William J. Martini, United States District Judge for the District of New Jersey, signed an order authorizing the interception of electronic communications occurring over the e-mail account of theodore dykstra@hotmail.com (hereinafter the "Dykstra Hotmail Account"). Actual interception pursuant to that order commenced on December 27, 2005. Over the following thirty day period, numerous pertinent e-mail communications were intercepted pertaining to individuals attempting to gain access to the "Illegal CP" website. Based on those interceptions, ICE agents have been able to determine the following:

i. The individual or individuals controlling the Dykstra Hotmail Account receives the information submitted by an individual attempting to subscribe to the "Illegal CP" website by some means or pathway other than the Dykstra Hotmail Account. That information includes the name of the subscriber,

the subscriber's address, the subscriber's credit card information and the subscriber's e-mail address.

ii. The individual or individuals controlling the Dykstra Hotmail Account then transmit this information via an attachment to an e-mail to one of the following e-mail addresses: joe777@mail.ru, admin@sib-games.com and admin@ad-soft.net. The Dykstra Hotmail Account then receives a return e-mail, typically on the same day, from one of the previously referenced e-mail accounts (joe777@mail.ru, admin@sib-games.com or admin@ad-soft.net) which effectively advises whether the individual should be accepted or rejected as a subscriber or whether some other action should be taken.[7]

iii. Finally, an e-mail from the Dykstra Hotmail Account is sent to the individuals whose credit card information has been satisfactorily verified

[7] Some individuals who attempt to subscribe have their credit card information reviewed by the operators of these e-mail accounts only to have these operators return their information to the operator(s) of the Dykstra Hotmail Account with a notation of "egold," which is a form of electronic payment. It is believed that many of these individuals have previously subscribed to the "Illegal CP" website and that the operators of the "Illegal CP" website typically require repeat subscribers to use this alternate form of payment, most likely because it is more difficult to track. The operators of the "Illegal CP" website offer a new subscriber who uses a credit card a subscription of 20 days' duration at a price of $79.99. Those who pay through e-gold are typically offered a subscription of 30 days' duration at a typical price of $40.00.

(a) informing them that they have been granted access to the "Illegal CP" website; (b) providing a password and login (typically those which have been previously selected by the would-be subscriber); and (c) supplying at least one link to the "Illegal CP" website. Accordingly, the interception of electronic communications over the Dykstra Hotmail Account provided direct evidence of those individuals who had successfully subscribed to the "Illegal CP" website.[8]

iv. In instances when the operator or operators of the Dykstra Hotmail Account desired that a would-be subscriber gain access to the "Illegal CP" website via E-Gold, an e-mail would be sent to that individual providing a link where the individual could access instructions for making payment through E-Gold. For those who were already able to make a payment through E-Gold, the e-mail listed one of two E-Gold accounts controlled by the operator or operators of the Dykstra Hotmail Account through which a subscriber could make a direct payment.

22. Interception of electronic communications over the Dykstra Hotmail Account ended pursuant to the December 23, 2005 order on January 25, 2006. Pursuant to an order signed by the Honorable William J. Martini authorizing continued interception

[8] Agents have discovered that the e-mail message notifying individual subscribers that they had been granted access to the "Illegal CP" website and would be billed by ADSOFT was not always sent via the Dykstra Hotmail Account. Agents have determined this by, among other things, execution of a search warrant relating to another e-mail account associated with the "Illegal CP" website which revealed the presence of similar messages which were not captured by the interception of electronic communications over the Dykstra Hotmail Account or via a trap and trace device relating to that account.

of electronic communications over the Dykstra Hotmail Account, interception resumed on or about January 27, 2006 and continued through February 25, 2006. During this time period, hundreds of individuals within the United States were granted access to the "Illegal CP" website.

23. During the period of authorized interception, ICE agents determined that the operator(s) of the "Illegal CP" website had shifted the contents of the website to a new server located in McLean, Virginia which began hosting the content of the website as early as December 2005. On or about February 1, 2006, a search of a server maintained by an ISP known as HopOne was conducted pursuant to a court-authorized search warrant. That search revealed the presence of thousands of images and videos of child pornography from the "Illegal CP" website contained on the server. In addition, numerous log files ranging from the period from October of 2005 through February 1, 2006 were recorded which documented contact by numerous IP addresses. These log files also included a variety of data of individuals who were members of the "Illegal CP" website including a member's ID, a member's login, the member's e-mail address and the date and time when the member's subscription began and the IP address. For each particular video or image which had been accessed by a member, the log files provided the member's ID, the IP address of the individual accessing the particular image and the date and time when that particular image had been accessed.[9] A second court-authorized

[9] The HopOne server did not provide log files for all dates during the relevant time period from December 2005 through early February 2006. For example, no log files are available for the time period from December 27, 2005 through December 30, 2005 and minimal log files are available from December 31, 2005 through January 2, 2006. In addition, it appears that some log files were deleted throughout the period of authorized

search warrant was obtained for this server on or about March 2, 2006 which provided log file information from February 1, 2006 through February 7, 2006, at which time the ISP shut down the website. The website was subsequently established on a third server after a disruption in access to the website which lasted several days, and which resulted in the operators of the "Illegal CP" website offering free access to archives of child pornography associated with the website to its inconvenienced subscribers.

24. During the course of the investigation, agents determined that the "Illegal CP" website offered access to a separate series of archives of child pornography videos which was labeled "BIG CP MOVIES." To obtain access to these archives, a subscriber would have to pay an additional fee, typically in the amount of $100.00. In addition, as previously mentioned, the contents of the main "Illegal CP" website were shifted between several servers between November 2005 and February 2006. During the period of authorized interception of electronic communications occurring over the Dykstra Hotmail Account,[10] access to the website was disrupted when the HopOne server was

---

interception by the operators of the "Illegal CP" website, but the reason for doing so is unknown.

[10] From the time when ICE agents originally purchased access to the "Illegal CP" website in October of 2005 through the end of the period of authorized interception over the Dykstra Hotmail Account in late February 2006, the design of the banner page of the "Illegal CP" website changed on numerous occasions - typically with new images of child pornography being added or subtracted from the page. However, the page always labeled itself "illegal.CP" and always featured images of child pornography on each of the more than 100 occasions during this four-month period when ICE agents visited the website. Agents also determined that other join pages were placed on the Internet through which a would-be subscriber could submit information for the purpose of gaining access to the "Illegal CP" website. Agents encountered and preserved two other join pages through which many of the subscribers gained access. One labeled itself "The Sick Child Room," and described its contents as featuring "the ultimate in child porn video." The other was

shut down in early February 2006. To placate subscribers who complained of this disruption, the operators of the Dykstra Hotmail Account offered subscribers free access to the archive of the subscriber's choice. As a result, a number of individuals who had a current subscription to the "Illegal CP" website at the time of the disruption in service sent e-mails informing the operator or operators of the Dykstra Hotmail Account specifying the particular archive to which they desired access. In response, an e-mail from the Dykstra Hotmail Account would be sent providing a link to the archive and a password.

25. Agents determined that the content of the "BIG CP MOVIE" archive was maintained by an ISP known as PiloSoft on a server located in New York City.[11] On or about April 21, 2006, a search warrant of this server was conducted pursuant to a Court-authorized search warrant. A review of the contents of this server revealed the presence of numerous videos of child pornography including many of those which had been advertised through the "Illegal CP" website and which had been offered as compensation to those whose subscribers who had experienced a disruption in access to the website in February of 2006. The server also contained log files which included, among other data, the subscriber's IP address, the particular file containing the archive to which the

---

entitled the "Children Porno Portal," and described itself as the "Kids Porn Archive." On every occasion when agents were able to locate and preserve these join pages, the pages used one of these labels and featured graphic images of child pornography, although the images might be changed over time.

[11] Agents have uncovered no evidence to suggest that the operators of HostDime.com, HopOne or PiloSoft were aware that their servers were being used to host a website offering access to child pornography.

subscriber had sought access, and the date and time when the subscriber's IP address had been used to gain access to the file in question.[12]

B. Probable Cause to Search the Subject Premises

26. ICE agents have determined that an individual named Brad Derrickson, who currently resides at the SUBJECT PREMISES, has subscribed to the "Illegal CP" website and has received child pornography. For the reasons set forth below, there is probable cause that

[12] During April and May of 2006, ICE agents based in Newark conducted four court-authorized search warrants on individual subscribers who resided in the State of New Jersey. Two of these individuals had been identified as successfully subscribing to the "Illegal CP" website through e-mails during the pendency of authorized interception of electronic communications over the Dykstra Hotmail Account, and agents had recovered log files from the HopOne server confirming that they had accessed images of child pornography during this time period. Another individual had been identified as successfully subscribing to the "Illegal CP" website in mid-February 2006 through intercepted e-mails but no log files were available to confirm his access to the website. Another individual had been identified as accessing images of child pornography during November 2005 through log files from the HostDime server, but he had not successfully subscribed to the "Illegal CP" website during the interception period. A review of the contents of computers seized during the execution of these search warrants revealed the presence of numerous images of child pornography on computers belonging to every one of these individuals.

evidence of the receipt and possession of child pornography will be located at the SUBJECT PREMISES.

27. On or about January 2, 2006, ICE agents intercepted the first of several e-mails transmitted over the Dykstra Hotmail Account which were relevant to the receipt and possession of child pornography by Brad Derrickson. At approximately 1:43 a.m. PST[13], the operator or operators of the Dykstra Hotmail Account sent an e-mail to joe777@mail.ru as an apparent request to verify the credit card and other information submitted by various individuals who sought subscriptions to the "Illegal CP" website. This data was included in an attachment to the e-mail which ICE agents were able to decode using commercially available software. Among those individuals seeking access to the website was an individual who listed his name as Brad Derrickson. He provided an address of [redacted] Dagsboro CT with a zip code of 19939. (Investigators believe the listing of Connecticut is erroneous and should be Delaware. The street address, city, zip code, and telephone number all listed in the attachment are specific to Delaware. Alphabetically, Connecticut is the state listed, immediately before Delaware. Investigators believe that when the state was listed the person at the keyboard used a drop-down list and erroneously missed Delaware by one entry.) He also listed his e-mail address as [redacted] and provided a telephone number of [redacted] He also provided a Delaware National Bank issued credit card number of [redacted] with a cvv number of [redacted] and listed the card's expiration date as January 2007. Also included in this data were his selected login of Unarie and his

[13] The times listed refer to the Pacific Standard Time when the email was received by the

selected password of 234432. In addition, the data from this e-mail included the IP address [redacted] from where Brad Derrickson had submitted his information, which was listed at [redacted], Dagsboro DE 19939.

28. January 2, 2006, at approximately 6:00 a.m. PST, ICE agents intercepted an e-mail message to the Dykstra Hotmail Account from joe777@mail.ru to the operators of the Dykstra Hotmail Account. This e-mail contained the e-mail addresses of numerous individuals seeking a subscription to the "Illegal CP" website and listed a variety of codes next to these addresses indicating whether, among other things, their credit card payment should be accepted or declined or whether they should be referred for payment through E-gold. For those for whom granting a subscription was advised, a notation of "term" followed by four or five digits was listed by their e-mail address. Within the list contained in this e-mail was the e-mail address for Brad Derrickson, namely, [redacted]n," followed by the notation "term 9257" indicating that his credit card payment should be accepted.

29. On or about January 2, 2006, at approximately 8:08 a.m. PST, ICE agents intercepted an e-mail message from the Dykstra Hotmail Account to the e-mail addresses of a number of individuals who had attempted to subscribe to the Illegal CP website. Among the recipients of this message was [redacted], the e-mail address of Brad Derrickson. The message informed the recipients that they had been granted access to the "Illegal CP" website by stating the following: "Hello. . . . !!!!!You have been billed by ADSOFT for 79.99!!!!!! This is a reminder of your membership at our site. Please visit

---

MSN Hotmail e-mail server located in California.

the memberzone or ask for a refund your money in a reply." The message then provided three links to the "Illegal CP" website, stating "For entering, use one of the these urls: http://mhumbu.badlink.net/ . . . http://pliac.hotfire.net/ . . . http://hualama.cjb.net

30. On July 27, 2006, a subpoena was sent to Delaware National Bank for credit card records of account number [redacted] This credit card number corresponds to the number for Brad Derrickson which had been sent in the email message from the Dykstra hotmail account to joe777@mail.ru on or about January 2, 2006. On July 28, 2006, investigators received the subpoenaed credit card billing records of Delaware National Bank from its VP/Security Officer. Those records confirmed that during the relevant period, Brad Derrickson, with a listed home address the same as the SUBJECT PREMISES, had a Visacheckcard in the same sixteen digit number referenced in the subpoena, and that the account had been billed $79.99 by "AD SOFT" with a transaction date of January 4, 2006.

31. On or about January 11, 2006, ICE agents using commercially available software determined that IP address [redacted] s controlled by Mediacom Communications Corp, 100 Crystal Run Road, Middletown NY 10941.

32. On or about March 9, 2006, representatives of Mediacom Communications Corp confirmed that the e-mail address of [redacted] subscribed to at the SUBJECT PREMISES. In addition, the Mediacom Communications Corp representatives related that the IP address of [redacted] is located at the SUBJECT PREMISES.

33. A check with the Division of Motor Vehicles on or about June 21, 2006, revealed that an individual named Brad Derrickson with a date of birth of [redacted] resides at the SUBJECT PREMISES.

34. A check with the Division of Motor Vehicles on or about June 21, 2006, revealed that a 2001 Ford Taurus with Registration Number [redacted] is registered to Brad Derrickson at the Subject Premises.

35. Based upon the information provided via the interception of electronic communications occurring over the Dykstra Hotmail Account, representatives of Mediacom Communications Corp, and surveillance of the SUBJECT PREMISES, there is probable cause to believe that the individual using the user or screen name [redacted] is Brad Derrickson, who lives at the SUBJECT PREMISES.

Specifics Regarding the Seizure and Searching of Computer Systems

36. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer forensic agents or experts in a laboratory or other controlled environment:

a. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, compact discs, and DVDs, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or

instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

37. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all

related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Conclusion

38. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess and/or receive child pornography, or attempt to do so, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, as described in Attachment B, are located at the SUBJECT PREMISES.

39. Based upon the foregoing, this Affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

David Yeary
Special Agent, ICE

Subscribed and sworn
before me this 9 day of August 2006

Honorable Mary Pat Thynge
United States Magistrate Judge